

Fact Sheet on the FTC's Commercial Surveillance and Data Security Rulemaking



Fact Sheet on the FTC's Commercial Surveillance and Data Security Rulemaking

Commercial surveillance is the business of collecting, analyzing, and profiting from information about people. Technologies essential to everyday life also enable near constant surveillance of people's private lives. The volume of data collected exposes people to identity thieves and hackers. Mass surveillance has heightened the risks and stakes of errors, deception, manipulation, and other abuses. The Federal Trade Commission (FTC) is asking the public to weigh in on whether new rules are needed to protect people's privacy and information in the commercial surveillance economy.

The Commercial Surveillance Industry

FTC enforcement actions, news reports, and published research indicate that the commercial surveillance industry is increasingly unavoidable. The FTC is concerned that companies have strong incentives to develop products and services that track and surveil consumers' online activities as much as possible. Companies refine their proprietary automated systems to better predict consumer behavior. Key features of the industry include:

- **Collection:** The FTC is concerned that companies collect vast troves of consumer information, only a small fraction of which consumers proactively share. Much of this data is collected through secret surveillance practices. Companies can track every aspect of consumers' engagement online. Companies can also surveil consumers while they are connected to the internet— their family and friend networks, browsing and purchase histories, location and physical movements, and a wide range of other personal details. Companies can collect data in other ways too, such as buying it from data brokers or pulling it from public sources.
- **Analysis:** The FTC is concerned that companies use algorithms and automated systems to analyze the information they collect. Companies can build consumer profiles and make inferences about consumers to predict their behavior and preferences. Companies may analyze this information without regard for the context in which it was collected.
- **Monetization:** The FTC is concerned that companies monetize surveillance in a wide variety of ways. Companies may use some of the information they collect to provide products and services, but they can also use it to make money. For example, they may sell the

information through the massive, opaque market for consumer data, use it to place behavioral ads, or leverage it to sell more products.

Commercial Surveillance Concerns

The FTC is seeking comment on a number of concerns stemming from commercial surveillance. These concerns include:

- **Lax Data Security:** The immense volume of information that companies collect and use requires a commensurate level of data security to keep it safe. However, the FTC is concerned that many companies do not sufficiently or consistently invest in securing the data they collect from hackers and data thieves. Despite widely accepted risk mitigation standards, they fail to use encryption techniques, and other protective measures.
- **Harms to kids:** Children of all ages are especially vulnerable to the deception and manipulation that can stem from commercial surveillance. There is a growing body of evidence that surveillance-based services are addictive to children and lead to a wide variety of mental health and social harms. With the expansion of technologies that are directed at kids and the education system's growing reliance on digital tools, children and teens face greater risks of immediate and long-term dangers.
- **Retaliation:** The FTC is concerned that many companies require people to sign up for surveillance as a condition for service. Companies may deny access to consumers who do not wish to have their personal information shared with other parties – or require consumers to pay a premium to keep their personal information private. These data practices, and the lack of meaningful alternatives, raise questions about whether consumers are really consenting.
- **Surveillance creep:** Some companies reserve the right to change their privacy terms after consumers sign up for a product or service. Consumers who want to maintain access may have no choice but to accept those updated terms, even those that materially break previous privacy promises. Companies may couch their updates in legal language that masks the new ways they will collect, analyze, and monetize consumers' information. They can then use data collected for one purpose for a wide variety of new purposes. And consumers may not have a way to say no.
- **Inaccuracy:** Very little is known about the automated systems and algorithms that analyze data. Companies do not publicly disclose how they work. Nor do they commonly offer consumers a chance to review or dispute the analysis. But research suggests that algorithms are prone to errors, bias, and inaccuracy. These flaws often stem from the design process, such as the use of unrepresentative datasets, faulty classifications, or flawed problem analysis, a failure to identify new phenomena, and lack of context and meaning.

- **Bias and discrimination:** Some commercial surveillance practices may discriminate against consumers based on legally protected characteristics like race, gender, religion, and age. Some companies may use these categories to deny consumers access to housing, credit, employment, and other critical services.
- **Dark patterns:** Companies increasingly employ dark patterns or marketing to influence or coerce consumers into choices they would otherwise not make, including purchases or sharing personal information.

FTC Rulemaking Process

Issuing the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking is the beginning of the FTC rule-writing process. It invites the public to provide input on (a) the nature and prevalence of harmful commercial surveillance practices, (b) the balance of costs and countervailing benefits of such practices for consumers and competition, and (c) proposals for protecting consumers from harmful and prevalent commercial surveillance practices. The comment period will be for 60 days following publication in the Federal Register.